Attorney Docket No. 9432-000084

Express Mail Label No. EK 218 565 935 US

Date October 22, 1999

10/22/99 1C525 U.S. 09/425592

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Hon. Commissioner of Patents and Trademarks
Washington, D. C. 20231

Sir:

Transmitted herewith for filing under 37 C.F.R §1.53(b) is a patent application for

ACTIVE DATA HIDING FOR SECURE ELECTRONIC MEDIA DISTRIBUTION

identified by: [ ] First named inventor _____
        or [X] Attorney Docket No. (see above)

1. **Type of Application**

   [X] This application is a new (non-continuing) application.

   [ ] This application is a [ ] continuation / [ ] divisional / [ ] continuation-in-part of prior
   application No. _____. Amend the specification by inserting before the first line the sentence:

       --This is a [continuation/division/continuation-in-part] of United States patent
       application No. _____, filed _____.--

       [ ] The entire disclosure of the prior application, from which a copy of the oath or
       declaration is supplied, is considered part of the disclosure of the accompanying
       application and is hereby incorporated by reference therein.

   If for some reason applicant has not requested a sufficient extension of time in the parent
   application, and/or has not paid a sufficient fee for any necessary response in the parent
   application and/or for the extension of time necessary to prevent the abandonment of the parent
   application prior to the filing of this application, please consider this as a Request for an Extension
   for the required time period and/or authorization to charge our Deposit Account No. 08-0750 for
   any fee that may be due. THIS FORM IS BEING FILED IN TRIPLICATE: one copy for this
   application; one copy for use in connection with the Deposit Account (if applicable); and one copy
   for the above-mentioned parent application (if any extension of time is necessary).

2. **Contents of Application**

   a. Specification of 19 pages;
         [ ] A microfiche computer program (Appendix);
         [ ] A nucleotide and/or amino acid sequence submission;

       [ ] Because the enclosed application is in a non-English language, a verified English
       translation [ ] is enclosed [ ] will be filed.

       [ ] Cancel original claims _____ of the prior application before calculating the filing fee. (At
       least one original independent claim must be retained for filing date purposes.)

   b. [X] Drawings on 4 sheets;

c. [X] A signed Oath/Declaration [X] is enclosed / [ ] will be filed in accordance with 37 C.F.R. §1.53(f).

The enclosed Oath/Declaration is [X] newly executed / [ ] a copy from a prior application under 37 C.F.R. §1.63(d) / [ ] accompanied by a statement requesting the deletion of person(s) not inventors in the continuing application.

d. **Fees**

FILING FEE	Number		Number			Basic Fee
CALCULATION	Filed		Extra	Rate		$760.00
Total Claims	20	– 20 =	0	× $18.00	=	0.00
Independent Claims	3	– 3 =	0	× $78.00	=	0.00
Multiple Dependent Claim(s) Used				$260.00	=	
FILING FEE – NON-SMALL ENTITY						760.00

FILING FEE - SMALL ENTITY: Reduction by 1/2 . . . .
      [ ] Verified Statement under 37 C.F.R. §1.27 is enclosed.
      [ ] Verified Statement filed in prior application.						

Assignment Recordal Fee ($40.00)						40.00
37 C.F.R. §1.17(k) Fee (non-English application)						
TOTAL						**800.00**

[X] A check is enclosed to cover the calculated fees. The Commissioner is hereby authorized to charge any additional fees that may be required, or credit any overpayment, to Deposit Account No. 08-0750. A duplicate copy of this document is enclosed.

[ ] The calculated fees will be paid within the time allotted for completion of the filing requirements.

[ ] The calculated fees are to be charged to Deposit Account No. 08-0750. The Commissioner is hereby authorized to charge any additional fees that may be required, or credit any overpayment, to said Deposit Account. A duplicate copy of this document is enclosed.

3. **Priority Information**

[ ] **Foreign Priority**: Priority based on _____ Application No. _____, filed _____, is claimed.

    [ ] A copy of the above referenced priority document [ ] is enclosed / [ ] will be filed in due course, pursuant to 35 U.S.C. §119(a)-(d).

[ ] **Provisional Application Priority**: Priority based on United States Provisional Application No. ____, filed ____, is claimed under 35 U.S.C. §119(e).

4. **Other Submissions**

[ ] A Preliminary Amendment is enclosed.

[X] An Information Disclosure Statement, one (1) sheet of PTO Form 1449, and eight (8) patents/publications/documents are enclosed.

[X] A power of attorney

    [X] is submitted [X] with the new Oath/Declaration.

    [ ] is of record in the prior application and [ ] is in the original papers / [ ] a copy is enclosed.

[X] An Assignment of the invention.

    [X] is enclosed with a cover sheet pursuant to 37 C.F.R. §§3.11, 3.28 and 3.31.

    [ ] is of record in a prior application. The assignment is to _____, and is recorded at Reel _____, Frame(s) _____.

[ ] An Establishment of Assignee's Right To Prosecute Application Under 37 C.F.R. §3.73(b), and Power Of Attorney is enclosed.

[X] An Express Mailing Certificate is enclosed.

[ ] Other: _____

_____

Attention is directed to the fact that the correspondence address for this application is:

    Harness, Dickey & Pierce, P.L.C.
    P.O. Box 828
    Bloomfield Hills, Michigan 48303
    (248) 641-1600.

    Respectfully,

Date OCT. 22, 1999
Harness, Dickey & Pierce, P.L.C.
P.O. Box 828
Bloomfield Hills, Michigan 48303
(248) 641-1600

    Timothy D. MacIntyre
    Reg. No. 42,824

HARNESS, DICKEY & PIERCE, P.L.C.
ATTORNEYS AND COUNSELORS
P.O BOX 828
BLOOMFIELD HILLS, MICHIGAN 48303
U.S.A

TELEPHONE
(248) 641-1600

TELEFACSIMILE
(248) 641-0270

Date: October 22, 1999

Hon. Commissioner of Patents
and Trademarks
Washington, D.C. 20231

Sir:

EXPRESS MAILING CERTIFICATE

Applicant:	Yu et al
Serial No. (if any):	To Be Assigned
For:	**Active Data Hiding For Secure Electronic Media Distribution**
Docket:	9432-000084
Attorney:	Gregory A. Stobbs / Timothy D. MacIntyre

"Express Mail" Mailing Label Number .... EK 218 565 935 US

Date of Deposit .... October 22, 1999

I hereby certify and verify that the accompanying check in the amount of $800 ($760 - basic filing fee; $40 - Assignment Recordal Fee); Transmittal Letter (in duplicate); 19-page patent application and executed Declaration and Power of Attorney; four (4) informal sheets of drawings (showing FIGS. 1-4); Recordal Cover Sheet (in duplicate) and Assignment; Information Disclosure Statement with Certificate of Mailing (4-pages); PTO-1449 with cited references listed therein (8 U.S. patents) are being deposited with the United States Postal Service "Express Mail Post Office To Addressee" service under 37 C.F.R. 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Barbara Goyke

**ACTIVE DATA HIDING FOR
SECURE ELECTRONIC MEDIA DISTRIBUTION**

Background and Summary of the Invention

The present invention relates generally to active data hiding, and more
particularly, to method and system for robustly hiding active data into a host
media data stream with errorless extractability.

Electronic media distribution imposes high demands on content
protection mechanisms for secure distribution of media. Average users are
starting to access and will soon be looking forward to purchasing multimedia
content through the Internet. This urges the development of secure content
distribution technologies with which content owners will agree to electronic
distribution of digital media such as video and audio. The problem is
amplified by the fact that the digital copy technology such as DVD-R, DVD-
RW, CD-R, and CD-RW are widely available. Accordingly, imperceptible data
hiding is becoming an attractive research area.

Previous research in the area of data hiding has been concentrated on
passive data hiding, such as digital watermarking, for copyright protection or
copy control. Passive data, as its name implies, can only be acted upon. In
other words, passive data cannot actively perform a task. Key renewal or
surveillance are two exemplary techniques for providing secure content
distribution. In the case of passive data hiding, this type of functionality can
only be achieved through additional functions built into the players. This
greatly limits the application domain and the renewability of the system when
additional functions are not available to the multimedia player devices.

1

Therefore, it is desirable to provide a method and system that can robustly hide active data into host media data stream with errorless extractability. Compared to conventional passive data hiding, active data hiding can improve renewability, controllability, and interoperability, provide additional application values and a higher level of security to electronic distribution of multimedia content.

For a more complete understanding of the invention, its objects and advantages refer to the following specification and to the accompanying drawings.

Brief Description of the Drawings

Figure 1 is a block diagram depicting an electronic media distribution system in accordance with the present invention;

Figure 2 is a flow diagram illustrating a method for hiding active data in accordance with the present invention;

Figure 3 is a flow diagram illustrating a method of decoding a host data signal embedded with an active data stream in accordance with the present invention; and

Figure 4 is a diagram depicting a perceptual mask in accordance with the present invention.

Detailed Description of the Preferred Embodiments

Data hiding is generally defined as imposing a meaningful, imperceptible and extractable data stream onto a host signal. Imperceptibility and extractability are two technical criteria for conventional data hiding.

5 Imperceptibility means that the embedded data needs to be hidden into the host data signal such that it will not interfere with the quality (e.g., visibility or audibility) of the host signal. In addition, the embedded data needs to be extractable from the host signal on a player device. The extracted hidden data can then be used for copy control, copyright protection and other

10 purposes.

In accordance with the present invention, active data hiding is a technique for hiding an applet or some other executable file into a host data signal. In addition to the imperceptibility and extractability requirements, active data hiding bears additional technical requirements. First, the size of

15 the active hidden data is usually at least several hundred bytes. Instead of low bit rate embedding as in the case of conventional passive data hiding, active data hiding requires high bit rate embedding. However, for a fixed size host signal, it is more difficult to hide additional hidden data into the host signal, and thus it is more difficult to satisfy the imperceptibility requirement.

20 Second, active data hiding requires blind detection capability for electronic media distribution applications. Since only the protected medium, is available to the playing device, the extraction of any hidden data has to be performed without the original host medium. Third, due to the sensitivity to errors in an executable file, the extracted active hidden data has to be virtually

25 errorless, i.e., the embedding has to be lossless.

An electronic media distribution system 10 is depicted in Figure 1. The media distribution system 10 includes a content provider device 12 that is connected via a distribution channel 14 to at least one player device 16. In operation, the original multimedia content is embedded with hidden data on

5   the content provider device 12. The embedded media is then transmitted through the distribution channel 14 to the player device 16. At the player device 16, the embedded multimedia content may be played or used. In addition, the hidden data may be extracted from the embedded data signal.

In accordance with the present invention, a method for hiding active

10   data in a host signal is shown in Figure 2. The host data signal is defined as original multimedia content, such as a digital video or audio signal. A preferred embodiment of the method uses a three-pass architecture to hide active data into a host data signal.

First, the host data signal is evaluated 22 to determine the media units

15   of the host data. For a digital video signal, the media unit is one or more frames of video data. The host data signal may be further evaluated to determine the type of features associated with each media unit. For instance, a frame of video data includes features such as objects, texture regions and background. This information is subsequently used to determine how to

20   embed the hidden data into the host signal.

The host data signal is then embedded with active hidden data, thereby forming an embedded data signal. Active hidden data is defined as a set of executable machine instructions, such as a JAVA applet or some other executable file or program. In order to embed the active data, the active data

25   stream is mapped 24 into a sequence of binary data. Although in the case of

4

a JAVA applet the active data stream is mapped into a sequence of binary data, it some instances it may not be converted to binary data. The bit stream of binary data is then inserted 26 imperceptibly into the host signal. It is also envisioned that the bit stream may be scrambled prior to insertion into the

5   host signal. Thus, the embedded data signal designates a modified version of the host data signal that has additional meaningful data embedded into it. Although the invention is not limited to a particular embedding scheme, base domain embedding and spectrum domain embedding are two exemplary embedding schemes.

10   The host data signal may also be embedded with hidden control data. Hidden control data is used to govern the use of the active hidden data. For example, hidden control data may include synchronization data, identification data, access control data, keys, management data, error correction data, authentication data or other types of control data. These various types of

15   control data are useful in the proper extraction of the active data stream as well as to control proper usage of the active data stream and the host signal. As will be more fully explained below, hidden control data is particularly useful to ensure errorless extraction of the active hidden data from the embedded data signal.

20   An additional embedding step is needed for each type of hidden control data embedded into the host signal. For illustration purposes, two types of control data are embedded into the host data signal in Figure 2: error correction data and authentication data. After generating the hidden control data in step 28, error correction data is first embedded 30 into the embedded

25   data signal. Subsequently, authentication data can be embedded into the

5

resulting data signal, thereby forming the embedded data signal that is to be transmitted to the player device.

Prior to being embedded into the host data signal, the active data stream may optionally be encrypted as shown at step 25. In this case, if the decryption key needs to be transmitted along with active data stream, the key may also be embedded in the control data.

Once the embedded data signal is received on the player device, a decoding process occurs as shown in Figure 3. As will be apparent to one skilled in the art, corresponding decoding techniques are performed to extract the embedded data signal received by the player device.

In this case, the authentication data is first extracted 40 from the embedded data signal. An authentication check is performed 42 to verify the reliability of the data signal. The active hidden data can the be extracted 44 from the embedded data signal.

Error correction data facilitates the extraction process of the active hidden data. Due to the additional control data hidden in the data signal, the detector/extractor on the player device can determine if there are any errors in the extracted active hidden data, and if so can further correct the errors such that the active hidden data is executable on the player device. The error correction process is shown at step 46. In this way, the present invention ensures errorless extractability of the hidden data.

At this point, the active hidden data can be executed 48 on the player device. Again, the active data stream may optionally be decrypted 47 prior to being executed on the player device.

In contrast to conventional passive data hiding, active hidden data introduces new functionality for ensuring secure electronic media distribution. For instance, an active data stream can be configured to permit feedback of information back to the content provider. In this case, when streaming or

5   online preview is performed over the distribution channel (e.g., the Internet) to the player device, the information is transmitted back to the content provider or the content distributor.

In other instances, the active data stream may be configured to allow a play-once-preview, to enable renew keys or other management rules, or to

10   scramble the host signal to prevent further unauthorized use of the content. These functions may be performed with the assistance of the hidden control data. For example, if an identification check or access control check fails, the host signal may be scrambled to prevent unauthorized use; otherwise the active data stream may perform other tasks while allowing authorized

15   playback/usage of the host signal.

A methodology for hiding active data in an audio signal is presented to further illustrate the principles of the present invention. In this case, a three-pass, multi-layer approach is used to embed active hidden data, error correction data and authentication data into an audio signal.

20   A first pass embeds the active hidden data into the host data signal. Proper usage of the perceptual model ensures the imperceptibility of the embedded hidden data. The perceptual model takes advantage of human auditory system's inability to distinguish noise under conditions of auditory masking. That is, the presence of a strong audio signal makes a temporal or

25   spectral neighborhood of weaker and imperceptible audio signals. Empirical

7

data shows that the human ear cannot distinguish the differences when a minor change is made on a singular point or maskee point (under the condition it is still a maskee point before and after the modification), where a singular point, masker point and maskee point are defined as follows:

5   • a singular point $I(j)$ is defined as iff sign $(I(j))$ = -sign($I(j-1)$) & sign($I(j)$)=-sign($I(j+1)$);

    • a masker point $I(j)$ is defined as a point with an intensity value larger than a threshold δ, i.e., amp($I(j)$)$\geq \delta$;

    • a maskee point $I(j^k)$ is defined as a point that is under the mask of a
10   masker point $I(j)$, i.e., amp($I(j^k)$) $\leq$ mask(amp($I(j)$))

To illustrate the above-described principle, a perceptual mask is graphically depicted in Figure 4. In this figure, sample a is a masker point and samples b, c and d are maskee points. While the following description applies the perceptual model to an audio host signal, it is readily understood that the
15 application of the perceptual model varies depending on the type of host data.

Furthermore, the application of the perceptual model also varies based on the particular embedding scheme being used to hide the active data. For instance, the masking ability of a given sample depends on its loudness in a base domain embedding scheme. In contrast, the masking ability of a given
20 signal component depends on its frequency position and its loudness in the spectrum domain embedding scheme. Empirical results further show that the noise masking threshold at any given frequency is solely dependent on the signal energy within a limited bandwidth neighborhood of that frequency and at any given time is solely dependent on the signal energy within a limited
25 temporal neighborhood. Accordingly, the base domain scheme has better

8

decoding performance in terms of speed than the spectrum domain scheme; whereas the spectrum domain scheme has higher survivability over compression than the base domain scheme.

As will be apparent to one skilled in the art, several techniques can be used to embed bits into the singular and maskee points of the host audio signal. For illustration purposes, a simple encoding technique is provided for embedding a sequence of bits Sb_1, Sb_2,...Sb_M into the singular bits $lsng_1$, $lsng_2$ ... $lsng_M$, of a host signal I_1, I_2,... I_n...I_N. The encoding technique is as follows:

- If $I(j)=0$, set $I(j)=I(j)+1$

- If the embedding bit Sb_m is 0 and the mth singular point is $lsng_m$, then set $lsng_1$ to 0.

- If the embedding bit Sb_m is 1, then leave $lsng_m$ unchanged or set $\varepsilon_1 \leq lsng_m \leq \varepsilon_2$, where ε_1 and ε_2 are lower and upper bound with ε_2 controlled by perceptual mark.

To ensure maximum detectability, error correction data and authentication data should be embedded into different data layers within the host data signal. The active hidden data layer and any subsequent control data layers are preferably orthogonal to each other. The orthogonality of the embedded layers avoids any interference between embedded bits, thereby ensuring extractability of each layer. For example, singular points and maskee points are two orthogonal features of the host data signal which may be used to hide different data layer. Accordingly, active data may be hidden in the singular points and the control data in the maskee points of the host signal. Alternatively, if the signal is partitioned into subsets or subspaces, then the features extracted from the different subsets or subspaces will be

9

orthogonal to each other. Thus, it is envisioned that other orthogonal aspects of the host data signal, such as other orthogonal features in the same domain (e.g., time, spectrum, etc.) or other features extracted from different orthogonal domains, may be used to embed the different layers. Although

5   orthogonality is preferred, it should be noted that different data layers may also be non-orthogonal as far as the zero false rate is guaranteed for the extraction of the active data stream.

Next, error correction data is embedded into the host data signal. Again, the error correction data is hidden in a second orthogonal layer of the

10   host signal. For illustration purposes, a 2D checksum error correction technique is being used to embed error correction data. Assume the error correction bit number is Q and the active data stream bit number is M. Thus, the error correction stream length (number of bits) satisfies $M=(Q/2)^2$ for the 2D checksum technique. For example, an active data stream having a length

15   of 4000 bits requires only $64 \times 2 \approx 128$ error correction bits in the case of 2D checksum. An exemplary 2D checksum technique is provided as follows:

- Let Q= ceiling[$2M^{1/2}$], i.e., let Q be the smallest integer which is no less than $2M^{1/2}$.

- Arrange Sb = $Sb_1, Sb_2, \ldots Sb_M$ into Q/2 chucks
20      $SB(1) = SB(1)_1, SB(1)_2, \ldots SB(1)_{Q/2} = Sb_1, Sb_2, \ldots Sb_{Q/2}$,
      $SB(2) = SB(2)_1, SB(2)_2, \ldots SB(2)_{Q/2} = Sb_{Q/2+1}, \ldots Sb_Q \ldots$ and
      $SB(Q/2) = SB(Q/2)_1, SB(Q/2)_2, \ldots SB(Q/2)_{Q/2} = Sb_{(QQ-2Q)/4+1}, \ldots Sb_M$

- Let $E_q= LSB(SB(q)_1+SB(q)_2+ \ldots +SB(q)_{Q/2})$ for $q \in (1, Q/2)$ and $E_q= LSB(SB(1)_q+SB(2)_q+ \ldots +SB(Q/2)_q)$ for $q \in (Q/2, Q)$,
25   where LSB(S) denotes the least significant bit of S.

While the above-described example employs a 2D checksum error correction technique, it is readily understood that other error correction techniques are within the scope of the present invention, including but not limited to Perfect

10

codes, Quasi-perfect code, Hamming code, Duel codes, Hadamard codes, Golay codes, Nordstrom-Robinson codes, BCH codes, Cyclic codes, MDS codes, Reed-Muller codes, Kerdock codes, Preparata codes, Quadratic-residue codes, Reed-Solomon codes, and Justesen codes.

5   Lastly, authentication data is embedded into the host data signal. Again, the authentication data is placed into a third orthogonal layer of the host signal. In this case, a preferred authentication scheme places the authentication value into the least significant bit of each sample of the host audio signal. To ensure orthogonality, ε_1 shall be set to 2 or larger for both

10   singular point and maskee point embedding of the authentication data. A overview of the authentication algorithm is as follows:

-      Choose verification block size B and dependent block size D (for example, B=128 and D=512 bits). Assume the host signal is a 16bits audio, concatenating all the high bits (all the bits except

15   the least significant bit) of the 512 samples yields a message Mb of 15x512=7680bits. By further concatenating a key of 512bits (or a key of shorter length which is padded to 512bits (or a key of shorter length which is padded to 512bits), a message MB of 8192bits is produced.

20   -   Computer the one way hash with the MD5 algorithm, MB'=h=H(MB) to generate a 128 bit message MB'. (Append time or other secondary hidden data, such as the error correction bits, host signal length, and/or owner information, if B> 128 bits.)

25   -   Use public key (or secret key, depends on different applications) cryptography method to sign MB' with secret key K creating MB''=Sgn(K, MB').

-      Insert the B bits message, MB'', into the least significant bit of each sample, from 1→0 if embedding 0 or 0→1 if embedding 1,
30   into the verification block.

A similar authentication scheme is further discussed in C.W. Wu, D. Coppersmith, F.C. Mintzer, C.P. Tresser, M.M. Yeung, <u>Fragile Imperceptible Digital Watermark with Privacy Control</u>, Proc. SPIE'99, vol. 3657.

5   The foregoing discloses and describes merely exemplary embodiments of the present invention. One skilled in the art will readily recognize from such discussion, and from accompanying drawings and claims, that various changes, modifications, and variations can be made therein without departing from the spirit and scope of the present invention.

Claims

1.   A method for distributing multimedia content in an electronic media distribution system, the media distribution device having a content provider device and at least one player device, comprising the steps of:

   providing active hidden data, where the active hidden data comprises a set of executable machine instructions;

   embedding active hidden data into a host data signal, thereby forming an embedded data signal;

   transferring the embedded data signal from the content provider device to the player device;

   extracting the active hidden data from the embedded data signal on the player device; and

   executing the active hidden data on the player device.

2.   The method of Claim 1 further comprising the steps of:

   providing control data that governs the use of the active hidden data;

   embedding the control data into the embedded data signal prior to transmitting the embedded data signal; and

   using the control data to ensure the errorless extractability of the active hidden data from the embedded data stream prior to executing the active hidden data on the player device.

13

3.   The method of Claim 2 wherein the step of embedding the control data further comprises embedding the control data orthogonal to the active hidden data in the embedded data stream.

4.   The method of Claim 3 wherein the orthogonal aspect of the host data signal are orthogonal features in the same domain or features extracted from two or more orthogonal domains.

5.   The method of Claim 2 further comprises the steps of:

defining at least a portion of the control data as error correction data;

extracting the error correction data from the embedded data stream after extracting the active hidden data; and

modifying the active hidden data using the error correction data prior to executing the active hidden data, thereby providing the set of executable machine instructions.

6.   The method of Claim 2 further comprising the steps of defining at least a portion of the control data as authentication data, and authenticating the embedded data stream using the authentication data prior to extracting the active hidden data.

7.   The method of Claim 1 further comprises the step of encrypting the active hidden data prior to embedding the active hidden data into the host data signal.

8.   A method for distributing active hidden data in an electronic media distribution system, the media distribution device having a content providing device and at least one player device, comprising the steps of:

providing active hidden data and control data, wherein the active hidden data comprises a set of executable machine instructions and the control data governs the use of the active hidden data;

embedding the active hidden data and the control data into a host data stream, thereby forming an embedded data stream

transferring the embedded data stream from the content providing device to the player device;

extracting the active hidden data from the embedded data stream on the player device;

using the control data to ensure the errorless extractability of the active hidden data from the embedded data stream; and

executing the active hidden data on the player device when the active hidden data is extracted without error from the embedded data stream.

9.   The method of Claim 8 wherein the step of embedding the active hidden data and the control data further comprises embedding the active hidden data orthogonal to the control data in the embedded data stream.

10.   The method of Claim 8 wherein the step of embedding the active hidden data and the control data further comprises using at least one of base domain embedding scheme or spectrum domain embedding scheme.

15

11. The method of Claim 9 wherein the orthogonal aspect of the host data signal are orthogonal signal features in the same domain or signal features extracted from two or more orthogonal domains.

12. The method of Claim 8 further comprises the steps of:

defining at least a portion of the control data as error correction data;

extracting the error correction data from the embedded data stream after extracting the active hidden data; and

modifying the active hidden data using the error correction data prior to executing the active hidden data, thereby providing the set of executable machine instructions.

13. The method of Claim 8 further comprising the steps of defining at least a portion of the control data as authentication data, and authenticating the embedded data stream using the authentication data prior to extracting the active hidden data.

14. The method of Claim 8 further comprising the steps of encrypting the active hidden data prior to embedding the active hidden data into the host data signal and decryting the active hidden data prior to executing the active hidden data on the player device.

16

15.   An electronic media distribution system for distributing active hidden data in a host data stream, the media distribution device having a content providing device and at least one player device, the content provider device comprising:

5   a bit stream generator receiving active hidden data and converting the active hidden data into an active bit stream, wherein the active hidden data comprises a set of executable machine instructions;

a first encoder receiving the active bit stream and the host data stream and embedding the active bit stream into the host data stream,
10   thereby forming an embedded data stream; and

a second encoder receiving control data and the embedded data stream and embedding the control data into the embedded data stream, wherein the control data is used to govern the use of the active hidden data.

16.   The media distribution system of Claim 15 wherein the second encoder embeds the control data orthogonal to the active bit stream in the embedded data stream.

17.   The media distribution system of Claim 15 wherein the orthogonal aspect of the host data stream are orthogonal signal features in the same domain or signal features extracted from two or more orthogonal domains.

17

18.   The media distribution system of Claim 15 wherein the first encoder embeds the active bit stream and the second encoder embeds the control data in accordance with either a base domain embedding scheme or spectrum domain embedding scheme.

19.   The media distribution system of Claim 15 wherein at least a portion of the control data is defined as error correction data and the correction module modifies the active bit stream using the error correction data, thereby providing the set of executable machine instructions on the player device.

20.   The media distribution system of Claim 15 wherein the player device comprises:

a first decoder receiving the embedded data stream and extracting the control data from the embedded data stream;

a second decoder receiving the embedded data stream from the first decoder and extracting the active bit stream;

a correction module receiving the active bit stream and the control data, and using the control data to ensure errorless extractability of the active bit stream from the embedded data stream; and

an initiator for executing the active bit stream on the player device.

ABSTRACT

A method is provided for distributing multimedia content in an electronic media distribution system. The method comprises the steps of: (a) providing active hidden data, where the active hidden data comprises a plurality of executable machine instructions; (b) embedding active hidden data into the host data stream, thereby forming an embedded data stream; (c) transmitting the embedded data stream from a content provider device to a player device; (d) extracting the active hidden data from the embedded data stream on the player device; and (e) executing the active hidden data on the player device.
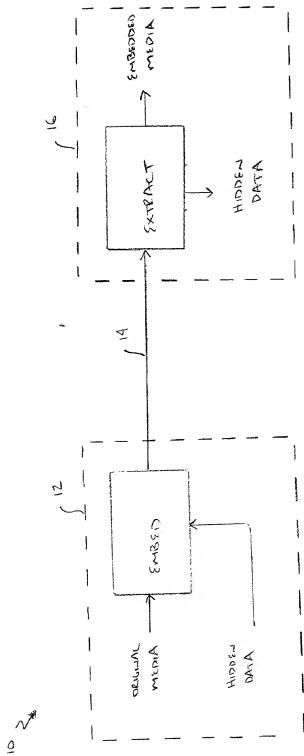
EMBEDDED
MEDIA

EXTRACT

HIDDEN
DATA

16

14

12

EMBED

ORIGINAL
MEDIA

HIDDEN
DATA

10

FIGURE 1

FIGURE 2

EVALUATE
HOST DATA   22

MAP ACTIVE
DATA TO   24
BIT STREAM

ENCRYPT
ACTIVE DATA   25
BIT STREAM

EMBED
ACTIVE   26
DATA

GENERATE
CONTROL   28
DATA

EMBED ERROR
CORRECTION   30
DATA

EMBED
AUTHENTICATION   32
DATA

```
┌─────────────────┐
│     EXTRACT     │ ──── 40
│     CONTROL     │
│      DATA       │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│  AUTHENTICITY   │ ──── 42
│     CHECK       │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│     EXTRACT     │ ──── 44
│     ACTIVE      │
│      DATA       │
└─────────────────┘
         │
         ▼
┌ ─ ─ ─ ─ ─ ─ ─ ─ ┐
│    PERFORM      │ ──── 46
│     ERROR       │          ┌────────────────┐ 47
│  CORRECTION     │ ─ ─ ─ ─ ▼│    DECRYPT      │
└ ─ ─ ─ ─ ─ ─ ─ ─ ┘          │  ACTIVE DATA   │
         │                   └────────────────┘
         ▼
┌─────────────────┐ ──── 48          │
│     EXECUTE     │ ◄ ─ ─ ─ ─ ─ ─ ─ ─┘
│     ACTIVE      │
│      DATA       │
└─────────────────┘
```
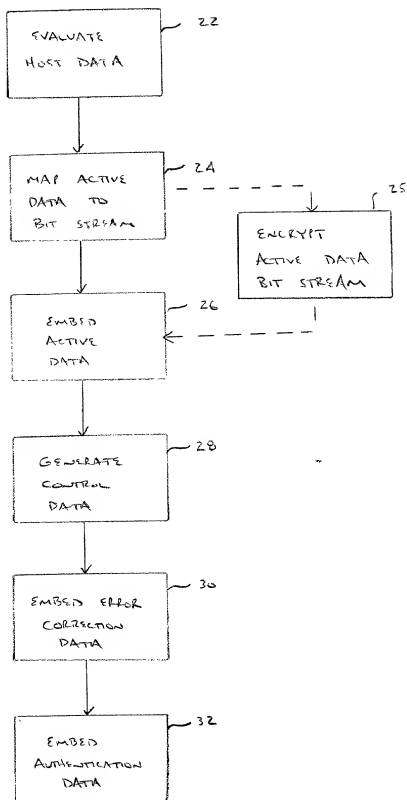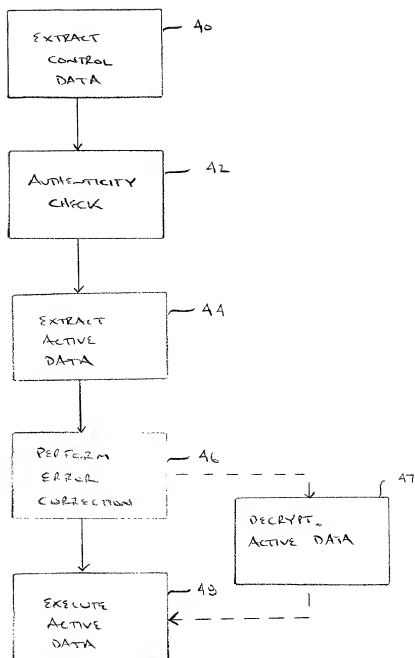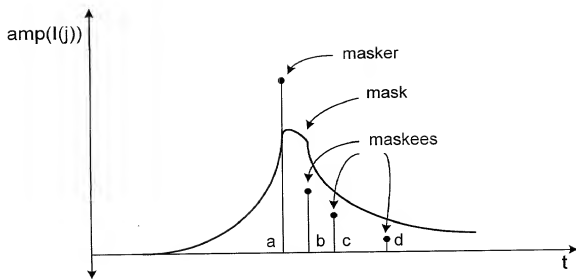
FIGURE 3

FIGURE 4

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled

ACTIVE DATA HIDING FOR SECURE ELECTRONIC MEDIA DISTRIBUTION

the specification of which (check one)

    [X]   is attached hereto.

    [ ]   was filed on _____ as Application

            Serial No. _____and was amended on

            _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

I acknowledge the duty to disclose information that is material to the patentability of the invention claimed in this application, or information that is material to the examination of this application, in accordance with Title 37, Code of Federal Regulations, section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, section 1190 (a)-(d) of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION (S)

Priority Claim

(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

DECLARATION AND POWER OF ATTORNEY

I hereby claim the benefit under Title 35, United States Code, §119(e) of any United States Provisional application(s) listed below:

PRIOR PROVISIONAL APPLICATIONS

(application serial number)	(Month / Day / Year filed)
(application serial number)	(Month / Day / Year filed)

I hereby claim the benefit under Title 35, United States Code, section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial No.	Filing Date	Status - patented pending, abandoned

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint Gregory A. Stobbs, Reg. No. 28,764, and each principal, attorney of counsel, associate and employee of Harness, Dickey & Pierce, P.L.C., who is a registered Patent Attorney, my attorney with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith. I request the Patent and Trademark Office to direct all correspondence and telephone calls relative to this application to Harness, Dickey & Pierce, P.L.C., P.O. Box 828, Bloomfield Hills, Michigan 48303 (248) 641-1600.

Full name of sole or first inventor: _Hong Heather Yu, Ph.D._

Inventor's signature: _____

Date: _____ _Oct. 20, 1999_

Residence: _28 Linden Lane, Plainsboro, New Jersey 08536_

Citizenship: _____ P.R.China

Post Office Address: _Same as above_

DECLARATION AND POWER OF ATTORNEY

Full name of second joint inventor, if any: Alexander D. Gelman, Ph.D.

Second Inventor's signature: _(signature)_

Date: _October 20, 1999_

Residence: 126 Coleridge Street, Brooklyn, New York 11235

Citizenship: US

Post Office Address: Same as above

Full name of third joint inventor, if any: Robert S. Fish, Ph.D.

Third Inventor's signature: _(signature)_

Date: 10 /20/99

Residence: 83 Cottage Place, Gillette, New Jersey 07933

Citizenship: US

Post Office Address: Same as above